Threat Convergence

by LTC Bill Flynt
Foreign Military Studies Office, Fort Leavenworth, KS.

This article appeared in

Military Review

September-October 1999

In this last annual threat assessment of the 20th century, I must tell you that US citizens and interests are threatened in many arenas and across a wide spectrum of issues. What is noteworthy is the manner in which so many issues are now intertwined and so many dangers mutually reinforcing.[1]

—George J. Tenet, Director of Central Intelligence

America faces unprecedented threats in type, location and scope. The threats span a universe from hacker intrusions into sensitive networks, to biological attacks by cults, to an impending, self-inflicted cyberstrike against critical infrastructures known as Y2K. The emerging threats all share one trait—regardless of motive or origin, they converge in targeting the US population and critical infrastructure.

Unfortunately, threat convergence directed at America's center of gravity has not lessened familiar threats. North Korea may explode, implode or both. China has made great strides in nuclear weapons and missile programs. Russia is nostalgic for past empire. Iraq still develops Weapons of Mass Destruction (WMD). However, several changes point out that new threats have fundamentally altered the security environment.

First, the trend of threat convergence signals the end of America's geographic sanctuary. Technology now enables adversaries to target America's population and critical infrastructure, a capability previously only the Soviet Union possessed. Exercise of this capability by those unhappy with the status quo may show that *in a single Superpower world, there is a single, best target*.

Second, because of these converging threats, we will increasingly fight from—and perhaps on—American soil. Power projection takes on a completely different meaning in the borderless worlds of terrorism, cyberspace, proliferation and economic espionage. Some of these threats will return past meaning to the oath, defend "against all enemies, foreign and *domestic*."

Third, intelligence and information requirements have converged as well. In a world where Latin American guerrillas finance war by selling drugs in the United States, smuggle Soviet arms from Eastern Europe and launder money through Caribbean banks for transfer into Swiss accounts, different intelligence efforts overlap.

A fourth difference from the Cold War's stark clarity is the effect of national security policy on domestic policies. During the Cold War America was threatened from beyond its shores, principally on foreign soil. With convergence, US threats are now outside, within and combined. Effective security policies against threats within US borders will affect domestic policies and politics. Ensuring security without risking liberty will prove difficult.

Each threat is unique in its means, ends and danger to the United States. All potential aggressors recognize that challenging the United States in a conventional, set-piece conflict risks defeat. If challenging America is required to advance their interests, they will prefer asymmetric, sometimes anonymous, attacks. A large-scale, direct challenge to US interests, such as Saddam Hussein's bid for Middle East dominance, is not a preferred *modus operandi*. American conventional and nuclear power, however, is impotent against a strategy of asymmetric conflict narrowly focused on a peripheral US interest. A fifth aspect of the security environment is that ideology is often meaningless. Hence, a strategy of asymmetric, anonymous attacks confounds US intelligence efforts, avoids US strengths and attacks its weaknesses and cannot be deterred.

Threat anonymity leads to a sixth distinction between the Cold War and present security environments—the potential of *Third-Actor Escalation*. Knowing that several states plan to launch cyber attacks in the early stages of conflict, diplomatic brinkmanship may be escalated by third actors, uninvolved in the conflict, launching strikes against the combatants. With its infrastructure under cyber attack, traced back to "spoofed" domains in the enemy's ministry of defense, a country may launch a cyber counterattack while it still has the capability.[2] Strangely enough, the dark logic of nuclear weapons, deterrence, counterforce and countervalue targeting, first-strike and second-strike capabilities has a renewed, profound meaning for cyber weapons in the 21st Century. However, unlike a nuclear arsenal, a cyberstrike can be launched by anyone.

Finally, a new threat's vital interest, or even existence, may rate only scant attention in intelligence reports. These threats are experts in narrow fields, where dominance means survival. Their growing number requires the United States to compete in an expanding arena of fields. These threats have few competing demands, unlike the United States. They may choose to do one thing well, unencumbered by traditional concerns of states. Attempting to meet every challenge would deplete even America's vast resources. Resource and analytical constraints and prioritized interests may force the United States to cede some battlefields.

In this altered security environment, America should choose its fights carefully. Emerging threats converge in targeting the US population and critical infrastructure. Denied a conventional, offensive response, the United States must rapidly adjust to defeat new threats. The first step is to understand the enemy.

The Threats

President Clinton addressed the potential use of cyber weapons or WMD against America's critical infrastructure, stating "it's sort of a balance thing, but I want to raise public awareness…without throwing people into an unnecessary panic."[3] The inclusion of both cyberstrike and WMD as dangers to the United States by the president indicates the convergence of various threats using completely different means.

Cyber weapons offer a small group the capability to disrupt social order. Stories of hackers entering sensitive networks are commonplace but generally attract little attention from those spared the effects—this is changing. Cyber weapons capable of disrupting the public sector are now commonplace and some are being used as mindless vandalism. In August 1998, a hacker angered by a chat room comment retaliated against Internet Alaska, the largest provider in the state. What began as a private matter between two people resulted in denied access for an entire region.[4] Society's increasing complexity and dependence on computers has spawned vulnerability. An individual can disrupt thousands of lives. Cyber weapons increasingly demonstrate some characteristics of WMD but without exclusive control by sovereign states.[5]

Whether the weapon is cyber, chemical, biological or radiological, the new threats may strike America's center of gravity. Where the intent is not to inflict casualties, as with espionage, the impact on national security can still be significant, as demonstrated by China acquiring America's most advanced miniature nuclear warhead technology.

Economic Espionage and Business Intelligence

> *The line separating purely economic intelligence from political intelligence is as difficult to draw as that between technical and military intelligence.*[6]
>
> —Louis J. Freeh, FBI director

The term business intelligence does not conform to a single definition. As generally used, business intelligence means timely information for decisions, competitive advantage as a result of knowledge, finding and using hidden relationships between data and improving predictions based on analysis. One opinion is, "Business Intelligence can be defined as collection of business and competitive information through legal and ethical methods."[7]

An example of "legal and ethical" business intelligence is the case of Pfizer Chemical Company. In 1996, Pfizer spent approximately $1.7 billion on research and development. One of their initiatives involved text-mining technology. They targeted biomedical documents in various databases, obtaining data on medical research projects. Pfizer describes the benefits as "higher productivity in research by making researchers aware of other projects and progress by other researchers." The author of this particular study, a data-mining consultant, offers a more explicit analysis, "We encountered at Pfizer a situation often found in the beginning usage of new and important technology. The company deems the system a competitive advantage and is reluctant to openly discuss too many of its particulars."[8] Clearly, business intelligence is important in today's competitive world.

However, the problem of using legal and ethical methods as the defining characteristic that separates business intelligence from economic espionage is that laws and ethics vary. French intelligence officers instruct business students at the *Universite Marne la Vallee* near Paris in the doctrine of the *Direction Generals de la Security Exterieure* (DGSE), France's intelligence service. Pursuing degrees in business intelligence engineering, the students are advised: "To recruit sources you've got to offer them something that interests them. To keep them firmly under control you need something that compromises or embarrasses them. To make them work

long and effectively on your behalf you need to treat them well and offer a reward or the hope of one."

Tools useful in controlling sources are "greed, revenge, job frustration, vanity and sex."[9] Competitive pressure guarantees that the legal and ethical perspective of business intelligence devolves to the lowest common denominator, with corresponding implications for the security of sensitive information. If there is a line between business intelligence and economic espionage, it centers on legal and ethical technicalities. That is a thin line for a frustrated insider recruited using the above techniques.

The United States only recently adopted legislation against threat economic espionage. Prior to the enactment of the *Economic Espionage Act of 1996*, "no Federal statute directly address[ed] economic espionage" comprehensively.[10] Until 11 October 1996, FBI agents investigated economic espionage by applying laws designed to counter interstate theft of physical property, such as cars, to combat the international electronic transmission of stolen data.[11] Attempting prosecution of those engaged in economic espionage involved creative use of statutes written for entirely different problems. Although the *Economic Espionage Act* is a potent law, its power is limited when dealing with foreign nationals operating outside the United States. The act does address conduct outside of the United States, stating that citizens and permanent resident aliens are covered under its provisions, as well as activity committed in the United States in furtherance of an offense.[12] However, this has no deterrent value against non-citizens hacking into "knowledge banks" from foreign soil.

Data and text mining enables the discovery and theft of information that a corporation may not realize it possesses. Mining software can automatically sift information from a remote location. Metadata, or information about data, yields patterns and details about the knowledge bank, such as frequency of word occurrence. If mining reveals high occurrence of a word, such as nuclear or microtoxin, the software can extract and flag relevant portions for human analysis. The analyst need not examine the entire contents of a database. Today, national intelligence agencies sift the Internet and penetrate computer networks, using text- and data-mining technologies to meet intelligence requirements. Research and development is a multi-billion dollar industry; even if not strictly defense related, it has security implications due to scientific and economic factors.[13] Today's archiving of literally all important data into knowledge banks makes data- and text-mining a powerful tool for economic espionage.

Computer defenses protect classified information, but that does not mean it is safe. Professional and state-sponsored hackers, enabled by an insider, can conduct espionage against national knowledge banks. The rigorous mining and analysis of numerous open sources and official-use sites can gather data that, when combined, approaches classified sources in quality. Multinational corporation or state-sponsored espionage teams can penetrate, establish a surreptitious presence and then monitor and sift incalculable numbers of databases, messages and web pages from beyond our shores. Their automated programs can key on such words as Aegis and satellite or monitor specific domains such as Raytheon or Pentagon. Because many database managers do not examine their databases critically, threats can know their knowledge banks better than they.

The Y2K Self-inflicted Cyberstrike

> *FEMA contingency plans are in draft form, but there is no national, strategic plan to assure that critical infrastructures will continue to function.*[14]
>
> —US Senate Report, February 1999

A threat consists of both the capability and intent to do harm. In the Y2K case, of course, there is no intent or actor. The Y2K cyberstrike is self-inflicted. However, the fact that Y2K is "launched" requires the same analysis of effects as if an actor had attacked.

Predictions regarding Y2K's effects range from scattered annoyances to the major failure of multiple critical infrastructure systems. Universal consensus indicates that *something* will happen—experts just differ on the degree. Most acknowledge some potential for widespread serious consequences. Mainstream organizations with reputations for balanced assessment, including the Red Cross and the Federal Emergency Management Agency (FEMA), are advising citizens to stockpile food, medicine, water, clothing and fuel.[15]

Analysts often miss a crucial point about Y2K's effects—the effects of Y2K may resemble those of a cyberstrike from a hostile state's information warfare team. Whether these effects are disastrous or merely unpleasant, Y2K demands preparation, response and consequence management. This potential matches a hostile cyberstrike in all aspects except timing.[16] Y2K is not an exercise—it is an acid test of readiness, involving real systems, with people and capital at risk. Its effects will be quantifiable. The consequences are unknown and could involve every sector of America's critical infrastructure. Paradoxically, Y2K may be a blessing.

Y2K provides an opportunity to evaluate critical infrastructure systems, computer net defenses and intergovernmental contingency plans under stress. It may expose deficiencies and could serve as a nationwide training exercise to prepare for strategic cyber attack.

However, Y2K also presents opportunities for malicious activity and exploitation. The most insidious will not be the hacks coinciding with New Year's celebrations, although these will cause damage. A dynamic industry provides Y2K solutions to corporations and companies in every business sector. The potential to exploit this one-time "in" for economic espionage and intelligence collection purposes is limited only by the imagination.

Hackers

> *We need to carry out what the government won't, and can't, do.*[17]
>
> —Legions of the Underground member

Hackers can defeat most computer defenses. The group "Hackers for Girlies" penetrated *The New York Times* on 13 September 1998 and posted a statement illustrated with nudes to protest the imprisonment of superhacker Kevin Mitnick. The *Times* fought to regain control of its servers for half a day.[18] Had profit or cause motivated the group, it could easily have established accounts within the system, seeded a backdoor Trojan Horse program such as "rootkit," and sold

a turn-key, high-profile cyberstrike capability to the highest bidder or donated it to a favorite terrorist organization.[19]

Traditional white-collar crime has turned to hacker techniques. The greatest threat to a corporation is the defection of a trusted insider who has constructed vulnerabilities for later exploitation. Hackers have stolen millions using cyber skills. Embezzlement can be accomplished remotely and the funds laundered electronically. Corporations victimized by electronic theft may be reluctant to pursue the thief or notify law enforcement officials, choosing instead to absorb the loss, correct the vulnerability and avoid public humiliation.

Hackers can cross the threshold of challenging national security, as evidenced by SOLAR SUNRISE, the February 1998 attack against DOD and other computer systems. This recent attack by cooperating teenage hackers in California, Canada and Israel illustrates the resources and knowledge required to mount a damaging cyberstrike are modest.

The ability to replicate a strategic cyberstrike makes *third-actor escalation* a characteristic of the new international security environment. During the Cold War, it was impossible for a third actor to "spoof" an incoming wave of intercontinental ballistic missiles during tensions between the superpowers. In today's security environment, hackers launching a cyberstrike could force states over the brink of war. With several countries possessing or developing cyberstrike capabilities and publicly declaring strategies of initiating future war with cyberstrikes, a third actor can escalate tensions at little cost and risk.

The hacker group "Legions of the Underground" (LoU) declared war against Iraq and China, due to their poor civil rights records. The group was not making an idle threat. It had previously successfully hacked the Chinese Human Rights web site, and in another unrelated operation, the same group had remotely hijacked a Time Warner Cablevision satellite dish.[20] In preparation for their announced cyberstrike, LoU conducted detailed reconnaissance and mapping of the Iraqi network, probing sequential network numbers and phone numbers to locate modems.[21]

Other hacker groups quickly condemned LoU's declaration of war and exerted pressure globally to halt the impending cyberstrike. The cyber diplomacy succeeded—LoU deigned to halt its critical infrastructure attack against Iraq and China. In the current security environment, autonomous hacker groups arrogantly and confidently debate whether to attack sovereign nations—and they have the means to do so. In the 21st century, hacker groups may exercise *de facto* veto powers.

Information Warfare Teams

> *A future war…may be triggered by a disruption to the network of the financial sector.*[22]
>
> —Wei Jincheng, PRC Strategist

In June 1997 the chairman of the Joint Chiefs of Staff directed a no-notice exercise, *ELIGIBLE RECEIVER 97* (ER97). The series of exercises was "designed to test DOD planning and crisis

action capabilities" against an attack on America's National Information Infrastructure (NII). The exercise revealed that a team of fewer than 30 people, with a nominal level of resources, can cause "considerable damage." The Director of the National Security Agency (NSA) stated that "strategic-level threat is technologically feasible today."[23]

Indications and warnings are impossible to detect until the preliminary stages of a cyberstrike. Distinguishing network reconnaissance by a single amateur hacker from coordinated surveillance by professional teams building a target folder is difficult.

Many nations are developing their Information Operations (IO) capability. The US is perhaps most advanced in IO—and most vulnerable. The infinite complexity and interdependencies of the NII offer countless entry points for information warfare teams. Hardening mission-critical systems and networks mitigates risk, but vulnerability remains exploitable through unforeseen, incomprehensible linkages. Charles Perrow states in addressing complex systems, "We have produced designs so complicated that we cannot anticipate all the possible interactions of the inevitable failures; we add safety devices that are deceived or avoided or defeated by hidden paths in the systems."[24]

The NII is complicated, and decades of cobbling together different hardware and software has produced a fragile system. Disruptions occur during routine operations, and although isolated parts of the NII can be hardened, an indirect attack cascading from unprotected systems may succeed. Mounting individual minor failures can cause catastrophic system failure. Perrow writes, "The cause of the accident is to be found in the complexity of the system. That is, each of the failures—design, equipment, operators, procedures or environment—was trivial by itself. …Though the failures were trivial in themselves, and each one had a backup system, or redundant path to tread if the main one were blocked, the failures became serious when they interacted. It is the interaction of the multiple failures that explains the accident."[25]

The NII's complexity makes mapping all interdependencies impossible. Critical systems need protection, but complexity makes failures inevitable. Contingency planning for post-cyberstrike consequence management should address major failures within the NII.

Information dominance is crucial to future security but may not be enough. The goal may be complete denial of enemy cyber communications. In future conflict the logic of first use may prevail: deny the enemy use of cyberspace before he denies us. Controlling cyberspace is like controlling the air, sea, land, space or electromagnetic spectrum. Information warfare teams are the frontline forces.

Cults

> *Well, uh, I think there was a religious group that committed suicide.*[26]
>
> — 911 call to San Diego county dispatcher

A cult can pose an asymmetric threat. It is a closed, potentially transnational group defined by internal beliefs and purpose. A cult may have no borders, no allegiance to nationality and may

reject mainstream societal norms. A cult leader's control can exceed that of highly disciplined terrorist organizations or elite military units. Cult leadership can dictate every aspect of a member's life, including schedule, diet, religious beliefs, activities, sex, marriage, child bearing and rearing, dress, education and ultimately, thoughts. Gaining acceptance within the cult requires increasing internalization of cult beliefs and norms; the recruit becomes an initiate, a member, and then a trusted operator. Progression between stages depends on demonstrated behavior under invasive supervision.

Penetrating a cult's higher levels is difficult because the informer must enter the cult as a recruit, and gaining access to information within the inner circle may take years, if it happens at all. In the process the informer may become a bona fide cult member or a double agent. Highly aware of surveillance techniques, a moderately sophisticated cult can defeat information-gathering efforts or manipulate perceptions to deceive outsiders. In open societies a large cult can escape attention by even its closest neighbors.

Every cult is unique. They exist across all conceivable categories and labels, including Oriental mysticism, voodoo and Celtic paganism. The Heaven's Gate cult believed that the Hale-Bopp Comet concealed a starship coming to take the members to a higher plane of existence, and the entire cult committed an elaborate ritual suicide to board the starship. A cult's belief determines its intent and, in turn, its threat to society. There are two components to cult intent influencing the degree of threat posed—the intent of members and the intent of cult leadership. Cult members can unwittingly serve the leadership's disguised intent and design. For example, members might donate all earthly wealth to achieve a higher plane of spirituality, but the cult leaders could use the collective wealth to finance terrorism, influence politics or acquire WMD.

President Clinton stated that the threat or use of a chemical or biological agent "is highly likely to happen sometime in the next few years."[27] In fact, there have already been small biological attacks in the United States, one of which involved a cult. This was the September-October 1984 poisoning of people in The Dalles, Oregon, by Bhagwan Shree Rajneesh's cultists.[28]

In the Rajneesh cult's operation, the leaders' intent was strictly political. They wished to minimize voter turnout and gain advantage in a local election they viewed as critical to their interests. Devout cultists spread *Salmonella Typhimurium* bacteria in 10 local restaurants, resulting in two different waves of outbreaks. The scale of the attack was significant—751 persons were infected. Implicated food items differed between restaurants, and investigation did not identify a common factor, such as a food distributor or water supply shared by the restaurants. So insidious is a biological attack, the fact it was a deliberate contamination was not discovered until about a year later.[29]

Another example of cult WMD use is Aum Shinrikyo. This cult had between 40,000 and 60,000 members around the world and assets of approximately $1 billion.[30] The cult was responsible for the 20 March 1995 Sarin gas attack on a Tokyo subway. However, less well known was the cult's successful infiltration of Japanese government and industry, including law enforcement and military organizations, and their development of a robust arsenal of chemical and biological weapons. Members had also used Sarin in at least one other attack and possibly a biological agent.[31]

WMD technology is readily available. Given the example of Aum Shinrikyo and the growing number of cults inspired by millennial, apocalyptic vision, future cult use of WMD is probable. Federal and state agencies should prepare for the consequences.

Paramilitary Organizations

> *The Federal Courts have become an imperial judiciary. In doing this, the courts have violated the sovereignty of the people.*[32]
>
> —Grievances Against the Federal Government

The Oklahoma City bombing focused US attention on paramilitary organizations. Although Timothy McVeigh did not represent any particular group, an increasing number of groups share his motives. The sophistication, resources, training, covertness and motives of these groups vary widely. Some are loosely organized associations of individuals with generally shared beliefs and interests. Others are organized, paramilitary cadres with advanced training, political doctrines couched in ideo-religious trappings, arsenals and plans for domestic terrorism against the federal government.

The more militant of these groups seek WMD for their arsenals. Ricin, an extremely lethal poison that is 6,000 times more potent than cyanide with no known antidote, was recently seized as evidence by the FBI from individuals involved in the Wisconsin militia movement. The amount of ricin, only seven-tenths of a gram of 4 percent purity, would have been sufficient to kill approximately 125 people. The intent was to use this highly lethal toxin as a WMD.[33]

A militia's level of training can be quite advanced. The larger groups pose a threat that exceeds the ability of law enforcement organizations to handle. Increasingly, these groups seek to influence local situations by filing property liens and harassing and intimidating their opponents.

The militia movement is not homogenous or centralized, which makes law enforcement intelligence efforts difficult. Different organizations pursue different objectives and have different vulnerabilities. Gaining intelligence to assess the actual threat of a specific group involves informers, undercover agents and surveillance of known members. This intelligence collection is a difficult and long-term task but essential in preventing domestic terrorism.

Terrorism and Extreme "Political Action" Groups

> *Bin Ladin's organization is just one of about a dozen terrorist groups that have expressed an interest in or have sought chemical, biological, radiological, and nuclear…agents.*[34]
>
> —George J. Tenet, Director Central Intelligence

Political extremism is not new. During the Cold War, organizations such as the Red Army Faction (RAF) committed acts of political violence. Other groups have supported independence

of ethnic regions, defeat of colonial masters and the overthrow of regimes. However, terrorism promoting interests below these levels of ideology, revolution, nationalism or freedom is new.

For example, the Animal Liberation Front (ALF) is a transnational group conducting violent advocacy of animal rights. Operatives work with and within other organizations including the Animal Rights Militia, the so-called Justice Department, Earth First! and the Earth Liberation Front (ELF). The nature of a planned operation dictates which group claims credit. Recently, the ELF claimed credit for the 18 October 1998 arson of a Vail, Colorado, ski resort, which caused $12 million in damage, stating the attack was conducted "on behalf of the lynx."[35]

The ALF uses arson, letter bombs, attacks on individuals, vandalism and public poisoning hoaxes. Its repertoire also includes cyberstrikes against companies doing animal research. The organization is a loose confederation of teams, using cyber-based, encrypted communications to evade law enforcement agencies. Their web presence includes propaganda, information operations and a cyberstrike unit called the Tactical Internet Response Network.[36] The ALF exemplifies a growing number of organizations using terror to support fringe causes. Common technology, not state sponsorship, equips these groups with capabilities potentially more lethal than the RAF possessed.

Terrorism, of course, still exists in today's security environment, but the use of terror has expanded horizontally (motive) and vertically (lethality). Terrorist groups now include those without political ideology as a cause. They are potentially more lethal with several pursuing a WMD capability. Some may achieve it.

Organized Crime and Transnational Criminals

> *Russian, Eastern European, and Eurasian criminal groups will pose a significant domestic problem for the U.S. in the future if they are not checked.*[37]
>
> —Louis J. Freeh, FBI director

Organized crime is a network of coordinated transnational sectors operated by regional crime societies. These sectors vary from trafficking in women and children to smuggling radiological and nuclear materials out of the former Soviet Union. In some countries, including Russia and Colombia, the power of criminal groups challenges the state's sovereignty.

Many of these international crime sectors pose direct threats to the United States. Counterfeiting, arms smuggling, transfer of dual-use and sensitive technologies, WMD proliferation, drug trafficking and money laundering all damage US interests. Criminal elements act freely in Central and Eastern Europe, Eurasia and other unstable regions. The rapid growth of criminal societies' power and the corruption of governments ensure "safe havens" for transnational operations that would have been impossible a decade ago.

For example, the official Russian news agency ITAR-TASS reported an incident of nuclear smuggling on 2 February 1999. According to the report, Turkish secret service agents had seized 100 grams of enriched uranium from four dealers who smuggled it into Turkey from Azerbaijan.

Describing the same incident the next day, the Turkish Anatolian agency reported that Turkish police had seized five grams of uranium, without mention of enrichment.[38] The discrepancy in the reported amount and quality of uranium seized is troubling from the proliferation perspective, but the main point is the increase in reported radiological and nuclear material smuggling.

The former Soviet Union is leaking nuclear and radiological materials onto a global market. Theft, covert distribution and international sale of nuclear and radiological agents is beyond the scope of petty crime; organized crime is marketing WMD knowledge and materials. It is a grave situation. "Between 1992 and 1994, there were at least seven unambiguous cases of diversion and recovery of weapons-usable nuclear material."[39] Reports indicate dozens of cases of radioactive isotope, low-enriched uranium, natural uranium and dual-use nuclear material smuggling between January 1995 and December 1997.[40] Although not confirmed by independent sources, there have been reported cases of additional loss of weapons-usable uranium from the Tomsk Polytechnical University in Russia, the Pacific Fleet naval base at Sovetskaya Gavan and the Vekua Institute of Physics and Technology in Sukhumi, Georgia.[41]

Organized crime has enabled terrorists to asymmetrically use nuclear agents. It is not known to what extent the former Soviet Union's nuclear inventory has been pilfered. Known incidents are attributed to "amateur criminals with no real buyers."[42] More sophisticated individuals may have attracted less attention and had more success.

> *It is a cause for serious, deliberate,disciplined, long-term concern.*[43]
>
> —William Jefferson Clinton

The current security environment presents a new reality. The most important US battlefields are no longer abroad—the Fulda Gap has been replaced by Indiantown Gap. New threats with varied motives from diverse origins converge along separate axes toward America's center of gravity—our population and critical infrastructure. The most sophisticated threats will combine cyberstrikes and WMD against our population and critical infrastructure, thus achieving a strategic countervalue deterrence capability previously only available to the Soviet Union.

The new threats alter the security environment but history should not be ignored. China, Russia or another may emerge as a future peer competitor, and there are still conventional threats abroad. However, they will avoid Iraq's past mistake in allowing the United States to assemble military might and embrace anonymous, asymmetric warfare using nontraditional weapons. President Harry S. Truman stated, "The world is not static, and the *status quo* is not sacred."[44] The challenge will be to stay ahead of the new threats' strategies already pursuing this truth.

---

1. George J. Tenet, Statement of the Director of Central Intelligence, George J. Tenet, as prepared for delivery before the Senate Armed Services Committee Hearing on Current and

Projected National Security Threats (Washington, DC: CIA, 2 February 1999). Document at <http://www.odci.gov/cia/public_affairs/speeches /ps020299.html.>

2. "Spoofing" is concealing cyber communications' true origin, while imitating a false origin.

3. White House Press Release, Interview of the President by *The New York Times* (Washington, DC: Office of the Press Secretary, 23 January 23 1999).

4. *USA Today*, "Hacker Blocks Internet Alaska Access" (Anchorage, AK: Associated Press, 25 August 1998) at <http://www.usatoday.com/life/cyber/tech/ctd333.htm.>

5. The director of Central Intelligence stated in testimony before the Senate Committee on Government Affairs on 24 June 1998 that a senior Russian official stated that cyberstrike effects overlap WMD. Testimony by Director of Central Intelligence, George J. Tenet, before the Senate Committee on Government Affairs 24 June 1998 (Washington, DC: Central Intelligence Agency Public Affairs Staff, 24 June 1998). Document at <http://www.cia.gov/cia/public_affairs/speeches/dci_testimony_062498.html.>

6. Louis J. Freeh, Statement of Louis J. Freeh, Director, Federal Bureau of Investigation, before the Senate Select Committee on Intelligence and Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology and Government Information Hearing on Economic Espionage (Washington DC: FBI, 28 February 1996). Document at <http://www.fbi.gov/archives/congress/econom/ecespion.htm.>

7. John F. Quinn, "Commercial Intelligence Gathering: Jetro and the Japanese Experience," a paper presented at the Fifth National OPSEC conference, "Managing Risk in the Information Age." (McLean, VA: National Security Institute, 2-5 May 1994). Document available at <http://nsi.org/Library/Intel/japanesp.html.>

8. Amy D. Wohl, *Intelligent Text Mining Creates Business Intelligence* (Narberth, PA: Wohl Associates, 26 February 1998), 4-5. Document at <http://www.software.ibm.com/data/pubs/papers/index.html#itmining.>

9. "Reality Lesson for Students," *Intelligence Newsletter: Business Intelligence, Technology, Threat Assessment*, no. 354, (Paris: Indigo Publications, 10 March 1999), 3. Document at <http://www.indigo-net.com/intel.html.>

10. Louis J. Freeh, Statement of Louis J. Freeh, Director, Federal Bureau of Investigation, before the Senate Select Committee on Intelligence and Senate Committee on the Judiciary, Subcommittee on Terrorism, Technology and Government Information Hearing on Economic Espionage (Washington DC: FBI, 28 February 1996). Document at <http://www.fbi.gov/archives/congress/econom/ecespion.htm.>

11. Ibid.

12. Title 18 of the *United States Code*, Chapter 90, Sections 1831 through 1839, 11 October 1996. Document at <http://www4.law.cornell.edu/uscode/18/ch90.html.>

13. Freeh, 5-6.

14. Investigating the Impact of the Year 2000 Problem, Report of the US Senate Special Committee on the Year 2000 Technology Problem (Washington, DC: US Senate, 24 February 1999), 2. Document at <http://www.senate.gov/~y2k/index.html.>

15. For representative disaster checklists from these organizations, see: The American Red Cross' Y2K preparedness checklist, 3 February 1999, at <http://www.redcross.org/disaster/safety/y2k.html> and the Federal Emergency Management Agency's checklist, 3 February 1999, at <http://www.fema.gov/pte/supplies.htm.>

16. The timing of Y2K is not simple. Several critical dates affect different systems in various ways. These dates are well documented in serious analyzes of the problem. Like a hostile cyberstrike, it is not a one-day event. Repercussions will likely contribute to the known timeline in unpredictable ways.

17. James Glave, "Crackers Set Sights on Iraq," *Wired Magazine*, 30 December 1998. Document at <http://www.wired.com/news/news/politics/story/17074.html.>

18. Amy Harmon, "Hacker Group Commandeers Times Web Site," *The New York Times* (14 September 1998).

19. "Rootkit" is a program that gains and maintains "root control" of a system. A Trojan Horse is a program disguised to appear innocuous. A "backdoor" is a surreptitious entry point or hidden vulnerability to entry into a system.

20. Glave, 2.

21. Ibid.

22. Wei Jincheng, "Information War: A New Form of People's War," *Liberation Army Daily* (25 June 1996), as appearing in Michael Pillsbury (ed.), *Chinese Views of Future War* (Washington, DC: National Defense University Press, 1997), 409.

23. LTG Kenneth Minihan, Statement of Lieutenant General Kenneth Minihan, USAF, Director, NSA, to the Senate Governmental Affairs Committee hearing on Vulnerabilities of the National Information Infrastructure (Washington, DC: US Senate, 24 June 1998), 2. Document at <http://www.senate.gov/~gov_affairs/62498minihan.htm.>

24. Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (New York: Basic Books, 1984), 11.

25. Ibid., 7.

26. Greg Lamotte, "Heaven's Gate 911 Call Eerily Calm" (Los Angeles: CNN, 18 April 1997). Document at <http://cnn.com/US/9704/18/cult.911/index.html.>

27. White House Press Release, Interview of the President by *The New York Times* (Washington, DC: Office of the Press Secretary, 23 January 1999).

28. Thomas J. Torok, MD, et al., "A Large Community Outbreak of Salmonellosis Caused by Intentional Contamination of Restaurant Salad Bars," *The Journal of the American Medical Association*, vol. 278, no. 5 (August 6, 1997), 389-395, and Shellie A. Kolavic, DMD, MPH, et al., "An Outbreak of Shigella dysenteriae Type 2 Among Laboratory Workers Due to Intentional Food Contamination", *The Journal of the American Medical Association*, vol. 278, no. 5 (6 August 1997), 396-398.

29. Ibid.

30. "Global Proliferation of Weapons of Mass Destruction: A Case Study on the Aum Shinrikyo," Senate Government Affairs Permanent Subcommittee on Investigations Staff Statement (Washington, DC: US Senate, 31 October 1995), section IV.C., Financial Operations.

31. Ibid., section II: Preliminary Findings & Questions.

32. The United States Theatre Command (a militia organization), "Grievances Against the Federal Government" (14 March 1999). Document at <http://www.eagleflt.com/list.html.>

33. US Department of Justice, Thomas Leahy of Janesville sentenced to over 12 years for possessing Ricin for use as a weapon, (Washington, DC: U.S. Department of Justice, 7 January 1998). Document at <http://www.usdoj.gov/usao/wiw/pr/wiw80107.2.html.>

34. Tenet, 3.

35. CNN, Group claims responsibility for Vail fires (Vail, CO: Associated Press, 22 October 1998). Document at <http://cnn.com/TRAVEL/NEWS/9810/22/vail.fire.01.ap/.>

36. "Animal Liberation Frontline Information Service," (April 1999). Document at <http://www.animal-liberation.net/.> See also <http://www.animal-liberation.net/tactical/index.html, and also http://floodnet.webjump.com/.>

37. Louis J. Freeh, International Crime: Prepared statement of Louis J. Freeh, Director Federal Bureau of Investigation, before the US Senate Committee on Appropriations Subcommittee on Foreign Operations (Washington, DC: FBI, 21 April 1998). Document at <http://www.fbi.gov/congress/intrcrime.htm.>

38. Andrey Palariya, "Turkish Secret Services Confiscate Enriched Uranium," Itar-Tass Information Service (Moscow: Itar-Tass, 2 February 1999).

39. Emily S. Ewell, "NIS Nuclear Smuggling Since 1995: A Lull in Significant Cases?" in *The Nonproliferation Review*, vol. 5, no. 3 (Monterey: Center for Nonproliferation Studies, Spring-Summer 1998), 119.

40. Ibid.

41. Ibid., 121.

42. Ibid., 122.

43. William Jefferson Clinton, remarks by the president on "Keeping America Secure for the 21st Century," a speech delivered to the National Academy of Sciences (Washington, DC: Office of the Press Secretary, 22 January 1999). Document at <http://www.pub.whitehouse.gov/uri-res/I2R?urn:pdi://oma.eop.gov.us /1999/1/22/9.text.1.>

44. Dean Acheson, *Present at the Creation: My Years in the State Department* (New York: W.W. Norton, 1969), 222.